

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI
SOUTHERN DIVISION**

ERICA WILLIAMS, et al.

§
§
§
§
§
§
§

PLAINTIFFS

v.

Civil No. 1:24-cv-24-HSO-MTP

SINGING RIVER HEALTH SYSTEM,
doing business as SINGING RIVER
GULFPORT, et al.

DEFENDANTS

**MEMORANDUM OPINION AND ORDER GRANTING DEFENDANTS’
MOTION [36] TO DISMISS FOR LACK OF JURISDICTION**

Defendants Singing River Health System, doing business as Singing River Gulfport, and Singing River Gulfport (collectively “the Hospitals”), seek dismissal of this case for lack of subject-matter jurisdiction. Because Plaintiffs lack standing to pursue their claims, the Court will grant the Motion [36] and dismiss Plaintiffs’ claims without prejudice for lack of subject-matter jurisdiction.

I. BACKGROUND

A. Factual Background

Defendants operate hospitals and other healthcare facilities in southern Mississippi. Compl. [32] at 8; Mem. [37] at 13. Plaintiffs assert that in August 2023, a ransomware gang known as “Rhysida” orchestrated a cyberattack on the Hospitals’ computer systems, gaining access to the personally identifiable information (“PII”) and protected health information (“PHI”) (collectively the “Private Information”) of Hospital employees and patients. See Mem. [38] at 3. As a result of this data breach (the “Data Breach”) Plaintiffs allegedly suffered various

injuries for which they seek damages, restitution, and injunctive relief. Compl. [32] at 1.

In their Consolidated Amended Class Action Complaint [32] (the “Complaint”), the named Plaintiffs to this suit are Erica Williams, Raymond Nox, Sabra Peterson, and Tara Dinkins, *id.* at 7-8; the Court will refer to each Plaintiff by their last name. Williams, Nox, and Peterson were all patients of Singing River hospital at the time of the Data Breach, and Williams was also an employee. *Id.* Dinkins brings this lawsuit on behalf of her minor child, who “she believes . . . *may have been treated at a clinic about ten years ago that was later acquired by Singing River.*” *Id.* at 38 (emphasis in original).

In the course of treatment or employment, Defendants required that each patient and employee provide various “sensitive, personal, and private” information (the “Private Information”). *See id.* at [32] at 10-11. Defendants also “create[d] and store[d] medical records and other protected health information, including records of treatments and diagnoses for its patients.” *Id.* On or around August 19, 2023, the Hospitals suffered a “malicious and sophisticated ransomware [attack]” on their computer systems, *id.* at 13, which “exposed the PII and PHI of hundreds of thousands of individuals, including Plaintiffs,” *id.* at 14.

On or about January 12, 2024, several months after discovering the Data Breach, Defendants began distributing notice letters to patients and employees “informing them that [Defendants’] investigation determined that their Private Information was accessed.” *Id.* at 15-16. These notice letters listed several “steps

that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity.” *Id.* at 16. Defendants also offered one year of credit monitoring to Data Breach victims. *Id.* This lawsuit followed.

B. Procedural History

Plaintiffs, individually and on behalf of all others similarly situated, bring claims for negligence, breach of implied contract, breach of fiduciary duty, invasion of privacy, and unjust enrichment, *see id.* at 48-60, request a declaratory judgment, *id.* at 60-62, and seek both damages and injunctive relief, *id.* at 1. In general, Plaintiffs claim the following types of injuries: (1) a loss of privacy due to the exfiltration of their Private Information; (2) being placed “at an actual, imminent, and substantial risk of harm from fraud and identify theft”; (3) being “forced to expend time dealing with the effects of the Data Breach”; (4) a “substantial and imminent risk of out-of-pocket fraud losses”; (5) the need to “incur out-of-pocket costs for protective measures”; (6) the “substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes”; (7) the diminution in value of their Private Information; and (8) being “forced to live with the anxiety that their Private Information . . . may be disclosed to the entire world[.]” *Id.* at 40-43.

Plaintiff Dinkins “received a Notice of Data Breach Letter regarding her minor child’s Private Information being accessed” during the Data Breach. *Id.* at 38. Dinkins “is uncertain whether her minor child was ever a patient of Singing River, but she believes the child *may have* been treated at a clinic about ten years

ago that was later acquired by Singing River.” *Id.* (emphasis in original). She is “uncertain why or how Singing River has her child’s Private Information.” *Id.*

Regarding injuries, Dinkins alleges that: (1) “she has to take extra measures to monitor the young teenaged child’s credit as well as her own”; (2) she is experiencing “great stress and anxiety”; (3) she experienced diminution in value of Private Information; (4) her—and her child’s—privacy rights were violated; and (5) she—and her child—are at risk of “present, imminent and impending injury arising from the increased risk of identity theft and fraud.” *Id.* at 38-39.

Plaintiff Williams—who was both a patient and employee of the Hospitals—alleges that her “name, date of birth, address, Social Security number, medical information, and health information” were stolen in the Data Breach. *Id.* at 32. As a result, Williams claims the following injuries: (1) that she is forced to spend about two hours per week monitoring her financial accounts to detect fraudulent activity; (2) that she suffers from “great stress and anxiety”; (3) that she was “specifically notified through Credit Karma and Experian that her personal information was found on the Dark Web”;¹ (4) that after the Data Breach she “began receiving an excessive number of spam calls and texts [and emails]” and had to change her cellphone number; (5) a violation of her right to privacy due to the exposure and

¹ “The dark web is an area of the internet accessible only by using an encryption tool. It provides anonymity and privacy online, and perhaps consequently, frequently attracts those with criminal intentions.” *United States v. Schultz*, 88 F.4th 1141, 1142 n.1 (5th Cir. 2023) (citing Gareth Owens & Nick Savage, *The Tor Dark Net*, The Global Commission on Internet Governance, Paper Series No. 20, 1 (2015)).

theft of her Private Information; and (6) that she “anticipates spending considerable time and money” mitigating the effects of the Breach. *See id.* at 31-33.

Plaintiff Nox—a patient of the Hospitals—alleges the following injuries: (1) actual fraud in the form of unauthorized charges on his checking account, most recently in about June 2024; (2) damage to and diminution in the value of his Private Information; (3) violation of privacy rights; and (4) “present, imminent and impending injury arising from the increased risk of identity theft and fraud.” *Id.* at 34-35. Additionally, Nox alleges that after the Breach, he “made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud.” *Id.* at 34.

Plaintiff Peterson—another patient of the Hospitals—alleges: (1) that she “discovered that she had fraudulent charge [sic] on her debit card, which required her to replace the card”; (2) that she “received notice from her Discover Card that her Private Information was found on the Dark Web”; (3) that she is forced to spend time monitoring her financial accounts closely; (4) that she suffers from stress and anxiety; (5) that she receives “an excessive number of spam calls on the same cell phone number that she provided to” the Hospitals; (6) a violation of privacy rights; (7) diminution in the value of her Private Information; (8) “present, imminent and impending injury arising from the increased risk of identify theft and fraud;” and (9) that she “is at a present risk and will continue to be at an increased risk of identity theft and fraud for her lifetime.” *Id.* at 36-37.

Defendants' current Motion [36] seeks dismissal of this action because "Plaintiffs lack Article III standing," and because the "Amended Complaint does not state plausible claims under Mississippi law." Mot. [36] at 1.

Regarding standing, Defendants argue that "Plaintiffs cannot satisfy the injury-in-fact requirement because they have not credibly alleged that, because of the Data Breach, they suffered actual or attempted misuse of their personal information resulting in actual loss or harm." Mem. [37] at 19-20. According to Defendants, Plaintiffs "only generally allege an increased risk of future harm in the form of potential identity theft or fraud," which is insufficient to confer standing. *Id.* at 20. Additionally, they contend that Plaintiffs have "failed to provide sufficient allegations to demonstrate traceability, *i.e.*, a sufficient causal connection between the injury and the conduct complained of." *Id.* at 25 (quotation omitted). This is because "[c]onsidering the ubiquitous nature of data breaches, Plaintiffs' failure to provide any credible allegations that the Private Information exposed by *this particular Data Breach* has been taken or misused" precludes a finding of traceability sufficient to support Article III standing. *See id.*

Defendants also assert that "there are no allegations that the Hospitals are somehow more likely than any other business to suffer another data breach or an attempted data breach in the near future," which means "Plaintiffs' claims for declaratory and injunctive relief must be dismissed" for lack of Article III standing. *See id.* at 26-27. In addition to their standing argument, Defendants contend that

Plaintiffs have failed to state a cause of action under Mississippi law. *See id.* at 27-28.

Plaintiffs respond that they have, indeed, each alleged a concrete injury sufficient to confer Article III standing. *See* Mem. [38] at 25-28. With respect to traceability, they assert that Defendants’ argument is procedurally premature in that it “attempts to insert an evidentiary standard at the pleading stage.” *Id.* at 28. Finally, Plaintiffs maintain that they have adequately stated a claim for relief under Mississippi law. *See id.* at 30-45.

II. DISCUSSION

A. Relevant Legal Standards

1. Motions to Dismiss under Federal Rule of Civil Procedure 12(b)(1)

Federal Rule of Civil Procedure 12(b)(1) permits a defendant to move to dismiss for “lack of subject-matter jurisdiction.” Fed. R. Civ. P. 12(b)(1). When considering such a motion, a court must “accept the complaint’s well-pleaded factual allegations as true,” *Carver v. Atwood*, 18 F.4th 494, 496 (5th Cir. 2021), and dismissal is appropriate “when the plaintiff does not ‘plausibly allege all jurisdictional allegations,’” *Ghedi v. Mayorkas*, 16 F.4th 456, 463 (5th Cir. 2021) (quoting *Brownback v. King*, 592 U.S. 209, 217 (2021)). “In other words, the same plausibility standard that applies in the Rule 12(b)(6) context also applies to Rule 12(b)(1).” *Id.* To evaluate a Rule 12(b)(1) motion, “a court may consider (1) the complaint alone, (2) the complaint supplemented by undisputed facts evidenced in the record, or (3) the complaint supplemented by undisputed facts plus the court’s

resolution of disputed facts.” *Tewari De-Ox Sys., Inc. v. Mountain States/Rosen Liab. Corp.*, 757 F.3d 481, 483 (5th Cir. 2014).

“For a 12(b)(1) motion, the general burden is on the party asserting jurisdiction.” *Dickson v. United States*, 11 F.4th 308, 312 (5th Cir. 2021) (citing *Castro v. United States*, 608 F.3d 266, 268 (5th Cir. 2010) (en banc)). As noted, Defendants have moved to dismiss under both Rule 12(b)(1) and 12(b)(6). *See* Mot. [36]. But “[w]hen a Rule 12(b)(1) motion is filed with other Rule 12 motions, the court should consider the Rules 12(b)(1) motion ‘before addressing any attack on the merits.’” *D&G Holdings, L.L.C. v. Becerra*, 22 F.4th 470, 474 (5th Cir. 2022) (quoting *Ramming v. United States*, 281 F.3d 158, 161 (5th Cir. 2001)).

2. Standing Generally

“Article III of the Constitution limits the jurisdiction of federal courts to ‘Cases’ and ‘Controversies.’” *Murthy v. Missouri*, 603 U.S. 43, 56 (2024) (quoting U.S. Const. art. III, § 2, cl. 1). “A proper case or controversy exists only when at least one plaintiff ‘establish[es] that [she] ha[s] standing to sue.’” *Id.* (quoting *Raines v. Byrd*, 521 U.S. 811, 818 (1997)) (alterations in original). Thus, to bring a lawsuit in federal court, plaintiffs must have standing, *Fed. Election Comm’n v. Cruz*, 596 U.S. 289, 295-96 (2022), which is a non-waivable, jurisdictional requirement, *La. Landmarks Soc., Inc. v. New Orleans*, 85 F.3d 1119, 1122 n.3 (5th Cir. 1996).

To satisfy Article III’s standing requirements, a plaintiff must demonstrate that she has “(1) suffered an injury in fact, (2) that is fairly traceable to the

challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citation omitted). “The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements.” *Id.* (citation omitted). And “[w]here, as here, a case is at the pleading stage, the plaintiff must ‘clearly . . . allege facts demonstrating’ each element.” *Id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 498 (1975)).

To satisfy the first element, an injury in fact, “a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Spokeo*, 578 U.S. at 339 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). For an injury to be “particularized,” it “must affect the plaintiff in a personal and individual way.” *Id.* And for an injury to be “concrete” it must be “‘*de facto*’; that is, it must actually exist,” *id.*, meaning it must be “real” and not “abstract,” *see id.* Although tangible injuries are easier to recognize, the Supreme Court has recognized that “intangible injuries can nevertheless be concrete.” *Id.* To determine whether an intangible harm constitutes an injury in fact, courts should “consider whether an alleged intangible harm has a close relationship to a harm that has been traditionally regarded as providing a basis for a lawsuit in English or American courts.” *Id.* at 341 (citing *Vermont Agency of Nat. Res. v. United States ex rel. Stevens*, 529 U.S. 765, 775-777 (2000)).

The requirement that an injury be “actual or imminent,” *Spokeo*, 578 U.S. at

339, means that the injury must have already occurred, be “certainly impending,” or be at “a substantial risk” of occurring, *Dep’t of Com. v. New York*, 588 U.S. 752, 767 (2019). Thus, “allegations of *possible* future injury” or theories of injury that rest “on a highly attenuated chain of possibilities” are not sufficient. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409-410 (2013) (emphasis in original); *see also Book People, Inc. v. Wong*, 91 F.4th 318, 329 (5th Cir. 2024) (“Injuries . . . that require guesswork as to how independent decisionmakers will exercise their judgment will not suffice.” (quotations omitted)). And in the case of a suit for damages, “the mere risk of future harm, standing alone, cannot qualify as a concrete harm” unless “the exposure to the risk of future harm itself causes a *separate* concrete harm.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 (2021) (emphasis in original).

To demonstrate traceability, Plaintiffs “must allege ‘a causal connection between the injury and the conduct complained of.’” *Book People*, 91 F.4th at 332 (quoting *Lujan*, 504 U.S. at 560). “Tracing an injury is not the same as seeking its proximate cause.” *Id.* But when the causal connection between the injury and the challenged action “depends upon the decision of an independent third party[,] . . . standing is not precluded, but it is ordinarily substantially more difficult to establish.” *Id.* (quoting *California v. Texas*, 593 U.S. 659, 675 (2021)). In such a circumstance, Plaintiffs “must show at the least ‘that third parties will likely react in predictable ways.’” *Id.* “A plaintiff cannot establish that an injury is ‘fairly traceable’ by proposing a ‘speculative chain of possibilities.’” *Williams v. Bienville Orthopaedic Specialists*, 737 F. Supp. 3d 411, 422 (S.D. Miss. 2024) (quoting

Clapper, 568 U.S. at 414).

To prove redressability, “Plaintiffs must show that a favorable decision will relieve a discrete injury to [themselves].” *Book People*, 91 F.4th at 332 (quotation omitted). It must be “likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Id.* (quoting *Friends of the Earth, Inc. v. Laidlaw Env’t Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000)).

3. Standing in Data Breach Cases

The Fifth Circuit has briefly considered standing in the context of a data breach. *See Ellis v. Cargill Meat Sols.*, No. 24-10339, 2024 WL 4692024, at *3 (5th Cir. Nov. 6, 2024) (per curiam) (“But Ellis only alleges the . . . cyberattack placed him at ‘continued risk of exposure to hackers and thieves of his’ [PII] and subjected him to ‘potential fraud and identity theft.’ He does not allege that risk has materialized. . . . Thus, Ellis fails to carry his burden here, too.” (citation omitted)). A number of other courts have had occasion to apply Article III standing doctrines in data breach cases. *See Williams*, 737 F. Supp. 3d at 417-20 (surveying Supreme Court and out-of-circuit precedent applicable to data breach cases).

Courts within the Fifth Circuit have applied standing doctrines in the data-breach context, and have arrived at varying conclusions. *See, e.g., Williams*, 737 F. Supp. 3d at 424-425 (holding that certain plaintiffs suffered an injury in fact but dismissing the complaint without prejudice because “[t]he mere fact that [plaintiffs] experienced misuse of their PII or learned that some of their PII had been stolen after the data breach is insufficient to show that the misuse of their PII is fairly

traceable to the . . . data breach”); *Hemphill v. Horne*, Civ. No. 3:24-cv-74, 2025 WL 837007, at *1 (S.D. Miss. Mar. 10, 2025) (“Of Hemphill and Chizek, only Chizek has plausibly pled injuries in fact based on the exposure of his private PII. All the same, the traceability requirement dooms his claims. That his private PII was exposed says nothing about whether it was exposed *in the breach*.” (emphasis in original)); *Logan v. Marker Grp., Inc.*, Civ. No. 4:22-cv-174, 2024 WL 3489208, at *1 (S.D. Tex. Jul. 18, 2024) (finding no standing where plaintiffs had failed to allege they were victims of actual identity theft, and holding that “even if Logan and Baxter’s alleged occurrences could constitute a sufficient injury-in-fact, they would still ‘fail to meet the causation and redressability elements of the standing test.’” (quoting *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015))); *Cabezas v. Mr. Cooper Grp., Inc.*, Civ. No. 3:23-cv-2453, 2025 WL 2053787, at *1 (N.D. Tex. Jul. 22, 2025) (finding standing because plaintiffs alleged injury in fact and because the traceability burden is “relatively modest at the pleading stage of the litigation” (quotation omitted)); *Merrell v. 1st Lake Properties, Inc.*, Civ. No. 23-1450, 2023 WL 6316257, at *4 (E.D. La. Sept. 28, 2023) (finding injury in fact and explaining that “Plaintiff has alleged that he does not recall receiving any other notices of data breach, and that his PII was compromised because defendant failed to implement minimum safeguards in contravention of its legal obligation to do so. At this stage, nothing further is required to establish traceability for constitutional purposes.” (citation omitted)). Nevertheless, the foregoing authority reflects that certain trends have emerged, which the Court finds persuasive.

First, as a general rule, courts in this Circuit—and others—have found that an increase in “spam communications do[es] not constitute an injury in fact.” *Cabezas*, 2025 WL 2053287, at * 5; *Williams*, 737 F. Supp. 3d at 421 (“However, Fendley’s allegation of an increase in spam phone calls is insufficient to establish an injury in fact.”); *Perklaki v. J.B. Poindexter & Co., Inc.*, Civ. No. 4:24-cv-01649, 2025 WL 754503, at *4 (S.D. Tex. Mar. 10, 2025) (Report and Recommendation) (“Accordingly, spam is not a concrete harm.”); *Hulse v. Acadian Ambulance Serv. Inc.*, Civ. No. 6:24-cv-01011, 2025 WL 1453847, at *8 (W.D. La. May 19, 2025) (Report and Recommendation) (explaining that “the Fifth Circuit would also likely consider an increase in spam email and text as a time-based injury insufficient to constitute a concrete injury”); *McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023) (“Spam calls, texts, and e-mails have become very common in the digitized world, and a number of courts have declined to confer standing when considering an increase in spam communications.”); *see also Hemphill*, 2025 WL 837007, at *8 (“Without more, Chizek seems to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls. This is not enough to infer that the [data] breach caused the spam communications.”); *In re ESO Sols., Inc. Breach Litig.*, Civ. No. 1:23-cv-1557, 2024 WL 4456703, at *5 (W.D. Tex. Jul. 30, 2024) (“Without specific facts linking the spam to ESO’s data breach, the increase in spam is not traceable to ESO.”).

Next, courts in this Circuit have generally viewed with disfavor theories of standing based upon diminution in value of PII or “loss of the benefit of the

bargain.” *See, e.g., In re ESO Sols., Inc. Breach Litig.*, 2024 WL 4456703, at *6 (“[D]istrict courts in Texas have been more skeptical [of diminution of PII claims], with at least three dismissing similar ‘loss-of-value’ claims. . . . Even if diminished PII was cognizable in the Fifth Circuit, Plaintiffs do not plausibly show their PII has diminished in value. Plaintiffs fail to allege that they attempted to or would have ever sold their PII. Nor do they allege that if they now attempted to sell their PII, they would be forced to accept a diminished price for it.” (internal citations omitted)); *Cabezas*, 2025 WL 2053287, at *6 (“Even if the Court found diminution of value a concrete harm, Plaintiffs fail to allege that they intended or attempted to sell their data and were forced to do so at a diminished price[;] the Court finds that they have not plausibly pled diminution of value.”); *Williams*, 737 F. Supp. 3d at 422 (“Finally, the named plaintiffs’ claims of injury-in-fact based on lack of benefit-of-the-bargain and diminished value of private information are not well-taken. There is no allegation that any of the plaintiffs paid a certain amount of money to Bienville in exchange for protection of their private information or that they intend to sell their private information.”); *Hemphill*, 2025 WL 837007, at *7 (“Hemphill and Chizek’s speculation that their PII’s value has diminished because it might have been stolen in the breach is not sufficiently concrete to satisfy the injury in fact requirement.” (quotation omitted)).

Finally, courts have reached varying conclusions about whether mere exposure of PII to unauthorized actors, without actual misuse, constitutes a concrete injury. The Second Circuit has held that mere exposure of PII is an injury.

See Bohnak v. Marsh & McClennan Cos., 79 F.4th 276, 285-86 (2d Cir. 2023) (“The core of the injury Bohnak alleges here is that she has been harmed by the exposure of her private information—including her SSN and other PII—to an unauthorized malevolent actor. This falls squarely within the scope of an intangible harm the Supreme Court has recognized as ‘concrete.’” (citing *TransUnion*, 594 U.S. at 424)). But the Eleventh and Fourth Circuits still appear to require some form of misuse before recognizing an injury in fact has occurred. *See Green-Cooper v. Brinker Int’l, Inc.*, 72 F.4th 883, 889 (11th Cir. 2023) (“We typically require misuse of the data cybercriminals acquire from a data breach because such misuse constitutes both a ‘present’ injury and a ‘substantial risk’ of harm in the future.” (citing *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021))); *O’Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023) (“[W]e’ve held that being subjected to a data beach isn’t in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft.”). Given the foregoing authority, the Court reaches several conclusions.

B. Plaintiffs have not Plausibly Alleged Standing to Support Their Claims for Monetary Relief

1. Plaintiff Dinkins has not Alleged a Concrete Injury-in-Fact

The Court begins with Dinkins, who asserts that: (1) “she has to take extra measures to monitor the young teenaged child’s credit as well as her own”; (2) she is experiencing “great stress and anxiety”; (3) she experienced diminution in value of Private Information; (4) her—and her child’s—privacy rights were violated; and (5)

she—and her child—are at risk of “present, imminent and impending injury arising from the increased risk of identity theft and fraud.” Compl. [32] at 38-39.

In the Court’s view, this is insufficient to allege an injury in fact because Dinkins has not claimed any actual misuse of her or her child’s Private Information. *See Perez v. McCreary, Veselka, Bragg & Allen, P.C.*, 45 F.4th 816, 824 (5th Cir. 2022) (“[I]f a risk hasn’t materialized, the plaintiff hasn’t yet been injured.”); *Green-Cooper*, 73 F.4th at 889 (“We typically require misuse of the data cybercriminals acquire from a data breach because such misuse constitutes both a ‘present’ injury and a ‘substantial risk’ of harm in the future.”); *Tsao*, 986 F.3d at 1343-44 (“[W]ithout specific evidence of *some* misuse of class member’s data, a named plaintiff’s burden to plausibly plead factual allegations sufficient to show that the threatened harm of future identity theft was ‘certainly impending’—or that there was a ‘substantial risk’ of such harm—will be difficult to meet.”); *O’Leary*, 60 F.4th at 244 (“In *Beck v. McDonald*, we held that plaintiffs whose personal information was compromised in a data breach hadn’t shown an Article III injury based on an alleged ‘increased risk of future identity theft and the cost of measures to protect against it.’” (quoting *Beck v. McDonald*, 848 F.3d 262, 267 (4th Cir. 2017))); *see also Williams*, 737 F. Supp. 3d at 421 (“[Plaintiffs] also have not alleged an injury-in-fact because they have not alleged misuse or actual access of their private information.”). And her assertion that she is forced to take extra measures to monitor her and her child’s credit are also insufficient, because “if the hypothetical harm alleged is not ‘certainly impending,’ or if there is not a substantial risk of the

harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk.” *Tsao*, 986 F.3d at 1339 (quoting and citing *Clapper*, 586 U.S. at 416).

Dinkins’s allegations of “great stress and anxiety,” Compl. [32] at 39, are likewise insufficient, absent an allegation of misuse or actual theft of the Private Information. *See Williams*, 737 F. Supp. 3d at 421-22 (“The Court further finds that these plaintiffs’ claimed mitigation expenses, anxiety, sleeplessness, and other forms of emotional distress are insufficient to establish standing in the absence of allegations of misuse or actual theft of the data.”). Further, Dinkins’s alleged injury based upon diminution in value of PII is not well taken; there is no assertion that Dinkins paid a certain amount of money to Defendants in exchange for protection of her child’s Private Information or that she intended to sell that information. *See, e.g., Williams*, 737 F. Supp. 3d at 422 (“Finally, the named plaintiffs’ claims of injury-in-fact based on lack of benefit-of-the-bargain and diminished value of private information are not well-taken. There is no allegation that any of the plaintiffs paid a certain amount of money to Bienville in exchange for protection of their private information or that they intend to sell their private information.”); *Hemphill*, 2025 WL 837007, at *7 (“Hemphill and Chizek’s speculation that their PII’s value has diminished because it might have been stolen in the breach is not sufficiently concrete to satisfy the injury in fact requirement.” (quotation omitted)). Because Dinkins has not alleged an Article III injury, she lacks standing to pursue her claims.

2. Plaintiff Williams has not Plausibly Alleged Article III Standing

Turning to Williams, most of her alleged injuries are, simply put, “too speculative to support standing,” *Ellis*, 2024 WL 4692024, at *3, because they rely on subjective fears of the *possibility* that a nefarious actor will defraud her. For example, Williams’s claim that she is forced to spend about two hours per week monitoring her financial accounts to detect fraudulent activity are insufficient because, although she has plausibly alleged that some of her information was published on the dark web, she has not plausibly alleged that any actual fraudulent activity is certainly impending or at substantial risk of occurring. And “if the hypothetical harm alleged is not ‘certainly impending,’ or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk.” *Tsao*, 986 F.3d at 1339 (quoting and citing *Clapper*, 586 U.S. at 416).

Williams’s claim that she “anticipates spending considerable time and money” mitigating the effects of the Breach, Compl. [32] at 33, is similarly unavailing because “allegations of *possible* future injury” or theories of injury that rest “on a highly attenuated chain of possibilities” are not sufficient. *Clapper*, 568 U.S. at 409-410 (emphasis in original). Nor does a claimed increase in spam calls, texts, or emails constitute an injury in fact. *See, e.g., Cabezas*, 2025 WL 2053287, at *5; *Williams*, 737 F. Supp. 3d at 421 (“However, Fendley’s allegation of an increase in spam phone calls is insufficient to establish an injury in fact.”). And the Court agrees with those courts holding that the mere exposure of Private Information,

without more, does not constitute an injury in fact. *See, e.g., O’Leary*, 60 F.4th at 244 (“[W]e’ve held that being subjected to a data breach isn’t in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft.”).

Finally, the Court is aware that some courts—including some in this Circuit—have held that publication of Private Information on the “dark web” constitutes an injury-in-fact. *See Green-Cooper*, 73 F.4th at 889 (holding plaintiffs’ allegations that personal information was exposed for theft and sale on the dark web was sufficient to establish an injury-in-fact); *Williams*, 737 F. Supp. 3d at 421 (same); *Cabezas*, 2025 WL 2053287, at *7 (same). But even assuming that is true, Williams has not plausibly alleged that the publication of her Private Information on the dark web was fairly traceable to Defendants’ alleged conduct. That is because even though Williams alleges that she “was specifically notified through Credit Karma and Experian that her personal information was found on the Dark Web,” Compl. [32] at 32, the Complaint [32] “provides no information linking the dark web posts with the [Defendants’] data breach,” *Williams*, 737 F. Supp. 3d at 3. In other words, Williams has not plausibly alleged “a causal connection between the injury and the conduct complained of.” *Book People*, 91 F.4th at 332 (quoting *Lujan*, 504 U.S. at 560). This is insufficient to confer standing.

3. Plaintiff Nox has not Plausibly Alleged Article III Standing

Turning to Plaintiff Nox, most of his alleged injuries are insufficient for reasons similar to those the Court has already articulated. Nox’s freestanding

claim for violation of his privacy rights does not confer standing because, as the Court has explained, the mere exposure of Private Information, without more, does not constitute an injury-in-fact. *See, e.g., O’Leary*, 60 F.4th at 244 (“[W]e’ve held that being subjected to a data breach isn’t in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft.”). And Nox’s assertion that he is at “increased risk of identity theft and fraud,” Compl. [32] at 35, is insufficient because that assertion is too speculative and because, as the Court has explained, “allegations of *possible* future injury” or theories of injury that rest “on a highly attenuated chain of possibilities” are not sufficient, *Clapper*, 568 U.S. at 409-410 (emphasis in original).

Similarly, Nox’s claim that he “made reasonable efforts to mitigate the impact of the Data Breach,” Compl. [32] at 34, do not confer standing because, although he has plausibly alleged he suffered unauthorized charges on his checking account, *id.*, he has not plausibly alleged that any additional fraudulent activity is certainly impending or at substantial risk of occurring. Nox cannot manufacture standing by responding to a hypothetical harm that may never materialize. *See Tsao*, 986 F.3d at 1339 (Explaining that “if the hypothetical harm alleged is not ‘certainly impending,’ or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk.” (quoting and citing *Clapper*, 586 U.S. at 416)). And even if this were enough to show a concrete injury in fact, Nox has not shown that his mitigation efforts are fairly traceable to *this* Data Breach.

Next, Nox's assertion that he has suffered damage to and diminution in the value of his Private Information, Compl. [32] at 35, is not well taken, *see, e.g., Williams*, 737 F. Supp. 3d at 422 ("Finally, the named plaintiffs' claims of injury-in-fact based on lack of benefit-of-the-bargain and diminished value of private information is not well-taken. There is no allegation that any of the plaintiffs paid a certain amount of money to Bienville in exchange for protection of their private information or that they intend to sell their private information." (internal citations omitted)); *Hemphill*, 2025 WL 837007, at *7 ("Hemphill and Chizek's speculation that their PII's value has diminished because it might have been stolen in the breach is not sufficiently concrete to satisfy the injury in fact requirement." (quotation omitted)).

That leaves Nox's final claim that he has "suffered actual fraud in the form of unauthorized charges on his checking account, most recently in about June 2024." Compl. [32] at 34. Although this is a concrete injury, it falls short because Nox has not plausibly alleged that the unauthorized charges on his checking account are fairly traceable to this Data Breach. *See Book People*, 91 F.4th at 332. As the *Williams* court recently explained

In today's society, an individual's PII and PHI can be stolen in myriad ways, often without the individual's knowledge. Data breaches and other forms of data theft are so prevalent that it is seemingly impossible to trace the misuse of personal information to one particular breach. The mere fact that [the plaintiffs] experienced misuse of their PII or learned that some of their PII had been stolen after the data breach is insufficient to show that the misuse of their PII is fairly traceable to the Bienville data breach.

Williams, 737 F. Supp. 3d at 425 (citing *Masterson v. IMA Fin. Grp., Inc.*, No. 2:23-cv-2223, 2023 WL 8647157, at *4 (D. Kan. Dec. 14, 2023) (“The only link between the data breach and the claimed misuse is that the misuse came after the data breach. This does not allege a substantial likelihood that the data breach caused the misuse.” (quotations omitted))).

Similarly, Nox has not asserted any additional facts which indicate that he suffered unauthorized charges on his account *because* of this Data Breach, nor has he adequately stated that any of his banking information was exposed in the Breach. *See* Compl. [32] at 34 (“Plaintiff Nox . . . was required to provide highly sensitive medical information and healthcare insurance information, most of which was and is protected by HIPAA.”); Ex. [32-1] at 3 (Nox’s Notice of Data Event) (“The investigation determined that the information potentially impacted *may* include your name, date of birth, address, Social Security number, medical information, and health information. We have no evidence that any of your information was used for identity theft or fraud.” (emphasis in original)). As far as the Court can tell, the only facts supporting a causal link between the Breach and the unauthorized charges is the fact that they occurred after the Breach. But in the Court’s view, this is insufficient to establish the requisite causal connection between the injury and Defendants’ conduct. *See Williams*, 737 F. Supp. 3d at 425 (“The mere fact that Williams, Schenck, and Rose experienced misuse of their PII or learned that some of their PII had been stolen after the data breach is insufficient to show that the misuse of their PII is fairly traceable to the Bienville data breach.”); *Masterson*,

2023 WL 8647157, at *4 (“The only link between the data breach and the claimed misuse is that the misuse came after the data breach. This does not allege a substantial likelihood that the data breach caused the misuse.” (quotation omitted)); *Hemphill*, 2025 WL 837007, at *9 (“Perhaps Chizek’s PII was stolen in the breach and misused, but Chizek has ‘not nudged’ those allegations ‘across the line from conceivable to plausible.’” (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007))). Nox has not plausibly alleged that he has standing to pursue his claims.

4. Plaintiff Peterson has not Plausibly Alleged Article III Standing

Peterson’s standing allegations are substantially similar to those made by the other named Plaintiffs. As noted previously, Plaintiff Peterson claims: (1) that she discovered fraudulent charges on her debit card; (2) that she received notice her private information was listed on the dark web; (3) that she spends time monitoring her accounts; (4) that she experiences anxiety; (5) that she receives excessive spam calls; (6) a violation of privacy rights; (7) diminution in the value of her Private Information; (8) “present, imminent and impending injury arising from the increased risk of identify theft and fraud;” and (9) that she “is at a present risk and will continue to be at an increased risk of identity theft and fraud for her lifetime.” *Id.* at 36-37.

Her claim that she discovered fraudulent charges on her debit card suffers from the same deficiencies identified in Nox’s assertions of unauthorized checking account activity—Peterson has not alleged any facts which plausibly indicate those charges occurred *because* of this Data Breach. Nor does she allege that any of her

banking or debit card information was even exposed in the Breach. *See* Compl. [32] at 36 (“The Notice Letter that Plaintiff Peterson received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the affected files contained her ‘name, date of birth, address, Social Security number, medical information, and health information.’” (quoting Ex. [32-1] at 4 (Peterson’s Notice of Data Event))). This is insufficient to demonstrate the requisite causal connection between the injury and Defendants’ conduct. *See, e.g., Williams*, 737 F. Supp. 3d at 425.

As for the jurisdictional deficiencies in each of Peterson’s remaining allegations, the Court has already addressed these. For the same reasons discussed *supra*, Peterson has not plausibly alleged standing.

C. Plaintiffs have not Alleged Standing to Support Their Claims for Declaratory or Injunctive Relief

The Court must separately address whether Plaintiffs have standing to seek declaratory and injunctive relief. *See TransUnion*, 594 U.S. at 431 (“[S]tanding is not dispensed in gross; rather, plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages).”). In sum, Plaintiffs ask the Court to: (1) enter a judgment declaring that Defendants owe—and continue to breach—a legal duty to employ reasonable measures to secure patients’ Private Information, Compl. [32] at 61; and (2) “issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols” to protect patients’ Private Information, *id.* Plaintiffs lack standing to request these forms of relief.

As the Fifth Circuit has explained:

Requests for injunctive relief and declaratory relief implicate the intersection of the redressability and injury-in-fact requirements. . . . Because injunctive and declaratory relief cannot conceivably remedy any past wrong, plaintiffs seeking injunctive relief can satisfy the redressability requirement only by demonstrating a continuing injury or threatened future injury. That continuing or threatened future injury, like all injuries supporting Article III standing, must be an injury in fact.

Stringer v. Whitley, 942 F.3d 715, 720-21 (5th Cir. 2019) (quotations omitted); *see also Book People*, 91 F.4th at 328 (“Plaintiffs seek injunctive relief, so they must show a continuing injury or threatened future injury, not a past one.” (quotations and citations omitted)). In particular, a plaintiff seeking injunctive relief must “show that it is likely, not merely speculative, that a favorable decision will redress the injury-in-fact” and “demonstrate either continuing harm or a real and immediate threat of repeated injury in the future.” *Gonzalez v. Blue Cross Blue Shield Ass’n*, 62 F.4th 891, 902 (5th Cir. 2023) (citation omitted). Therefore, the pertinent inquiry is whether “the risk of harm is sufficiently imminent and substantial.” *TransUnion*, 594 U.S. at 435 (citing *Spokeo*, 578 U.S. at 341-42).

In this case, Plaintiffs lack standing to pursue declaratory or injunctive relief because they have not alleged facts “tending to show that a second data breach is currently impending or there is a substantial risk that one will occur.” *Williams*, 737 F. Supp. 3d at 426 (quoting *Hummel v. Teijin Auto. Techs., Inc.*, No. 23-cv-10341, 2023 WL 6149058, at *14 (E.D. Mich. Sept. 20, 2023)); *see also Cabezas*, 2025 WL 2053287, at *8 (“While Plaintiffs have pled that Mr. Cooper retains their data and are able to identify security measures that could be improved, this claim for

injunctive relief is based entirely on the speculative risk of a second data breach.”); *Beck*, 848 F.3d at 277-78 (“The most that can be reasonably inferred from the Plaintiffs’ allegations regarding the likelihood of another data breach . . . is that the Plaintiffs *could* be victimized by a future data breach. That is not enough.”). Plaintiffs’ requests for declaratory and injunctive relief should be dismissed for lack of standing.

III. CONCLUSION

Because Plaintiffs have not plausibly alleged Article III standing, the Court is without subject-matter jurisdiction to entertain this matter, and their claims should be dismissed without prejudice. To the extent the Court has not specifically addressed any of the parties’ remaining arguments, it has considered them and determined that they would not alter the result.

IT IS, THEREFORE, ORDERED AND ADJUDGED that, Defendants Singing River Health System, doing business as Singing River Gulfport, and Singing River Gulfport’s Motion [36] to Dismiss for Lack of Jurisdiction is **GRANTED**.

IT IS, FURTHER, ORDERED AND ADJUDGED that, Plaintiffs Erica Williams, individually and behalf of all other similarly situated, Raymond Nox, Sabra Peterson, and Tara Dinkins’s claims against Defendants are **DISMISSED WITHOUT PREJUDICE** for lack of subject-matter jurisdiction. The Court will enter a separate Final Judgment in accordance with Federal Rule of Civil Procedure 58.

SO ORDERED AND ADJUDGED, this the 28th day of August, 2025.

s/ Halil Suleyman Ozerden

HALIL SULEYMAN OZERDEN
CHIEF UNITED STATES DISTRICT JUDGE